INCIDENT REPORTING SYSTEM AND METHOD

5   BACKGROUND OF THE INVENTION

1.   FIELD OF THE INVENTION

The present invention relates to a computer-based method of collecting and processing incident reports filed by witnesses who observe incidents such as criminal acts and legal violations. The method automates the collection and processing

10   of the incident reports and automatically sends the incident reports to the appropriate authority so that the observed incidents can be acted on in an appropriate manner.

2.   DESCRIPTION OF THE PRIOR ART

Citizens frequently observe criminal acts, legal violations, and other

15   incidents that they wish to report to the appropriate authority or authorities. However, many people do not know who the appropriate authority is or how to contact them and therefore either report the incident to the wrong authority or fail to report the incident at all. Even when people know who the appropriate authority is, they often decide not to report their observations for fear of getting involved in a criminal matter.

20   The 911 emergency telephone system has been developed in the United States to provide a convenient way for citizens to report emergencies. However, this system is intended for use in emergencies only, not for reporting incidents in general. Moreover, the 911 system is geographically limited in that each city or zone in the country must set up and operate its own emergency phone system. Moreover, 911

25   systems are expensive to operate because they rely upon human operators. Another problem with reporting incidents by telephone is that witnesses often fail to provide complete information about their observations because they are excited or in a hurry, making it difficult for the appropriate authority to accurately act on the observations.

30   OBJECTS AND SUMMARY OF THE INVENTION

The present invention solves the above-described problems and provides a distinct advance in the art by providing a computer-based method for receiving, collecting, and processing incident reports provided by witnesses. The method broadly

includes the steps of receiving into a computer system an incident report from a witness who observed an incident committed by an offender; prompting the witness to provide certain types of information about the incident; selecting an appropriate authority to whom the incident report should be sent; and sending the incident report to the selected

5   authority so that the authority can respond to the incident report. In preferred forms, additional information is added to the incident report either automatically by the computer system, by the authority to whom the incident report was sent, or by other persons who are allowed to access the incident report by way of a publicly searchable database.

10   The present invention encourages witnesses to submit incident reports because it allows them to remain anonymous and does not require them to know or identify to whom the incident report should be sent. Moreover, the invention improves the accuracy of incident reports because it does not rely upon human operators to collect the information and automatically prompts the witness to provide certain types

15   of information about the incident that is needed to properly act on the incident. The invention further improves the reporting and processing of incidents by adding additional information to the incident report from other sources based on the information entered into the report by the witness to automatically obtain a more complete report of the incident.

20

BRIEF DESCRIPTION OF THE DRAWING FIGURES

A preferred embodiment of the present invention is described in detail below with reference to the attached drawing figures, wherein:

Fig. 1 is a schematic representation of computer and communications

25   equipment used to implement some of the steps of the present invention; and

Fig. 2 is a flow chart illustrating the primary steps of the invention.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

As illustrated in Fig. 1, the method of the present invention is preferably

30   implemented with a central computer 10, a plurality of user computers 12, and a communications network 14 for routing communications therebetween. The central computer is preferably a conventional file-server microcomputer such as those

manufactured by Digital Equipment Corporation. The central computer includes conventional memory, input and output ports, and a modem or other communication device and is operable for receiving, storing and retrieving data and files as described below.

5   The user computers 12 are preferably personal computers such as IBM compatible microcomputers containing Intel Pentium type microprocessors but may also be "dumb" terminals with communication capabilities. Each user computer includes conventional memory, input and output ports, a modem and software for communicating with and interpreting data sent from the central computer 10. Those skilled in the art will

10   appreciate that any number of user computers may be used with the present invention.

        The communications network 14 is preferably a conventional telecommunications network including a plurality of switches connected to corresponding local exchange carriers. The network may also be a local area network, wide area network, wireless network, voice network, or any other type of network operable for

15   coupling the user computers 12 to the central computer 10. Private communications may be encrypted or otherwise protected before being transmitted over the communications network using available technology.

        Those skilled in the art will appreciate that the method of the present invention may be implemented with virtually all types of hardware and that the preferred

20   central computer 10, user computers 12 and communications network 14 are described merely to set forth one best mode of the invention.

        The method of the present invention is preferably implemented with a computer program that controls the operation of the central computer 10. The computer program may be stored in the read-only-memory (ROM) or hard drive memory of the

25   central computer or on conventional external disks for transfer to the memory of the central computer. The data records including the incident reports associated with the method of the present invention are preferably stored in the hard drive memory of the central computer.

        The computer program interface is preferably written in a Standard

30   Generalized Mark-up Language (SGML) such as Hypertext language. The mark-up language cooperates with a standard server language such as Common Gateway Interface (CGI) or Practical Extraction and Report Language (PERL) for handling the

various operating functions of the central computer 10. Those skilled in the art will appreciate that the computer program can be written in other computer languages as a matter of design choice.

5   The steps in the method of the present invention are broadly illustrated in Fig. 2. The method permits a person who witnesses an incident to report the incident so that it can be acted on by the appropriate authority. The incident may be a criminal act such as the commission of a robbery, a legal violation such as a traffic violation, a consumer offense such as the sale of a defective product or the rendering of an unsatisfactory service by a business or restaurant, or any other observation made by a

10   witness that the witness wishes to report. As described below, several witnesses may report information regarding the same incident.

The method begins when a witness uses one of the user computers 12 to contact the central computer 10 via the communication network 14 to report an incident. The initial access depicted in step 100 may include conventional log-on or connection

15   for data transfer procedures. The central computer 10 then displays or transmits an initial message to the appropriate user computer 12 describing the function and capabilities of the automated incident reporting system.

The computer program operating the central computer 10 next prompts the witness to fill out a complete incident report so that the central computer can process the

20   report as depicted in step 102. For example, the program preferably prompts the witness to enter the time and date the incident occurred, a full description of the incident, several key words that best describe the incident such as "robbery", "speeding violation", or "bad service", the exact or general location of the incident, and an indication of whether physical or financial harm was done to the witness or others The program may

25   also prompt the witness to identify which law or rule the witness believes was violated as a result of the incident, or the program may automatically identify which law or rule was violated based on the other information entered by the witness or from other information such as information from past incident reports or even data that is collected independently by the system such as by video surveillance equipment.

30   The program also preferably prompts the witness to identify any other potential witnesses who may also have observed the incident. If other potential witnesses are identified, the central computer attempts to contact them via the

communications network and requests that they complete a separate incident report as described above. If other potential witnesses submit additional incident reports, all of the incident reports are combined into a single case as described in more detail below.

To encourage the entry of accurate and honest information, the program

5   may also ask the witness if he or she is willing to testify that the entered information is true and accurate and asks the witness if he or she is willing to be contacted about the incident report. To encourage the use of the incident reporting system by persons who do not wish to be known, the program also allows witnesses to remain anonymous, to designate portions of their witness report that they do not want disclosed to others, or

10   to identify certain persons such as the perpetrator of the incident who they do not want to allow access to the incident report.

After the incident report has been fully completed, the program next prompts the witness to identify the offender or perpetrator of the incident as depicted in step 104. For example, when the incident is a criminal act or legal violation committed

15   by an offender, the program preferably prompts the witness to enter identifying information such as the offender's name, address, physical description, license plate number, phone number, etc. Similarly, when the witness is a complaint against a company or other entity, the program preferably prompts the witness to enter identifying information such as the company's name, address, phone number, etc.

20   The program then attempts to make a positive identification of the offender based on the information entered by the witness. For example, if the witness enters the name and address of the offender, the central computer may access proprietary or publicly available databases such as phone directories, government databases, or Internet directories to confirm that the identified offender actually exists and that the

25   information entered by the witness is accurate. The program may also use the information entered by the witness to collect additional identification information from these databases to supplement the incident report as depicted in step 106. If additional information is found, the program displays the information to the witness and prompts the witness to confirm that the correct person has been identified.

30   If the witness was not able to enter the name, address, or other information that would permit a positive identification of the offender, the program may access the above-described databases in an attempt to gather additional information that would

permit a positive identification. For example, if the witness merely entered physical description information and the general vicinity of the incident, the program may search databases to identify persons who match the physical description and that live in the general vicinity of the incident. The program then displays a list of all persons matching

5   the entered description, possibly including photographs of the persons, and asks the witness if any of the persons is the offender.

Even if the witness does not enter enough information and the program cannot discover enough additional information to permit a positive identification of the offender, the above identification processes are performed to obtain as much

10   information as possible regarding the offender and to possibly narrow the list to include certain characteristics. For example, the identification process may narrow the list of suspected offenders to include only caucasian males between the ages of 30 and 40 that are under 6' tall. As described in more detail below, this information may be used in connection with other information to make a positive identification of the offender.

15   The program may also supplement the incident report with other useful information such as addresses, names, etc. For example, if the witness reported an incident involving a company in a particular city but did not know the exact address and phone number of the company, the program may search the above-described databases to obtain the exact addresses and phone number of the company.

20   Each time the program supplements the incident report, the central computer 10 sends the supplemented incident report to the witness so that the witness can once again verify the accuracy of the report as depicted in step 108. If the witness wishes to further modify the report, the steps described above may be repeated as depicted in step 110.

25   After the witness and the program have entered all possible information into the incident report, the authority to whom the incident report should be sent is selected as depicted in step 112. The authority may be a local police department or prosecutors office, the FBI, CIA or other federal or governmental agency, a consumer group like the Better Business Bureau or any other group or agency that regularly

30   receives such information.

The authority may be selected by the witness, automatically by the program, or a combination of the two. For example, if the witness observes a criminal

activity such as a robbery, he or she may request that the incident report be sent to the local police. Or, if the witness does not know who the appropriate authority is, the program may automatically select the authority based on the information entered by the witness. For example, if the incident report involves a traffic violation, the program may

5   automatically send the report to the traffic violations bureau of the local police. Similarly, if the witness requests to send the incident report to a particular authority such as the local police, the program may evaluate the information entered by the witness and determine that the incident report should also be sent to another authority such as the FBI.

10   The program next contacts the appropriate authority via the communications network 14 and sends or otherwise makes the incident report available to the authority as depicted in steps 114 and 116. The authority may then supplement the incident report based on the information entered by the witness and the program to make the incident report more complete as depicted in step 118. The supplemented

15   information may include information that is contained in proprietary databases available only to the authorities.

In addition to notifying specific authorities, the program may enable a witness to indicate that their report may be accessible by any and all qualified authorities. Interested authorities can then search the program for any and all reports

20   that they are qualified to receive.

After the authority has supplemented the incident report, the authority is requested to send the supplemented report back to the central computer 10. Alternatively, the authority may be requested to supplement the report while on-line with the central computer 10 so that the master copy of the incident report always remains

25   on the central computer. The central computer then sends or otherwise makes available to the witness the supplemented incident report as depicted in step 120 so that the witness can once again verify the accuracy of the report, especially the supplemented information. If the witness wishes to further modify the report, the steps described above may be repeated as depicted in step 122.

30   The authority then acts upon the incident report in a conventional manner as depicted by step 124. For example, the authority may build a case against the

offender and arrest or penalize the offender once the authority has sufficient information and believes that the incident report involves a punishable matter.

The central computer 10 periodically contacts the authority through the communication network 14 to inquire whether the authority has acted on the incident report and to obtain information regarding the action taken. This information is then added to the incident report as depicted in step 126. The program and the central computer 10 may also allow authorities to rule or take action on an incident report while on-line. For example, if the selected authority is a police officer or judge, that police officer or judge can review the incident report along with all other supporting reports as described below and then post a decision or issue an arrest warrant that is posted on a file in the central computer.

The program may also prompt the authority to enter a fine or judgment against the offending party in response to the authority's decision regarding the incident report. The program then automatically contacts the offending party and instructs the offending party how to pay the fine or meet the obligations of the judgment. The program may post the fine or judgment on a publicly searchable database as described below and may monitor whether the fine is paid or judgment is satisfied. If the offender who must pay the fine is a registered user as described below, the program may automatically debit the user's account in the amount of the fine.

The central computer 10 and corresponding program are also configured to permit third parties to obtain information about incidents reported by witnesses. To this end, and as depicted in step 128, the central computer stores incident reports in a publicly-searchable database to enable persons to monitor incidents in their communities and to encourage more witnesses to add information to an incident report. For example, if numerous persons witness an incident, the first witness to access the central computer 10 will file an incident report as described above. Then, as additional witnesses access the central computer to file an incident report, the central computer will recognize, based on the information entered, that the new incident reports involve the same incident as the first filed incident report. The central computer will then combine the information entered by the various witnesses into a single case and then allow all the witnesses to access the information in the case. This results in a more complete description of the incident because the information entered by one witness

may refresh the memory of another, and vice versa, thus resulting in more accurate and complete incident reports.

The central computer 10 and corresponding computer program may also provide a warning system that alerts users to certain dangerous conditions based on

5   incident reports and other information that has been previously entered and stored into the system. For example, if numerous incident reports have been filed regarding criminal activities in a certain geographic area, the central computer identifies this trend and posts a notice on a searchable database alerting persons who access the central computer to avoid the geographical area.

10   The computer program is also configured to encourage or discourage witnesses from submitting reports by predicting the outcome of an incident before the incident has actually been handled by a selected authority. To this end, the computer program may compare the information entered into an incident report to the information entered into past incident reports that have already been resolved. If the new incident

15   report has similar facts as past incident reports, the program alerts the witness that he or she is likely to obtain a similar outcome as the past, similar incidents.

In addition to allowing and encouraging witnesses to file incident reports, the present invention may obtain information regarding incidents by other means such as with surveillance cameras to supplement the incident reports and to provide

20   confirmation of the observations of the witnesses. Use of video surveillance for compilation of information allows the gathering of information without requiring disclosure of certain personal information to other users. For example, a witness may be equipped with a video input system such as a personal surveillance camera and a display. When the witness encounters an incident such as a suspect committing a

25   crime, the video input system would automatically recognize the suspect from the video input and could then display records for the suspect on the witness's hand held readout without revealing the suspect's identity. The witness would not need to know the identity of the suspect to observe the incident relating to the suspect. Such a system may overcome some of the problems associated with publicly revealing personal data.

30   To encourage the input of accurate and honest information regarding incidents, the central computer 10 may require that witnesses become registered users of the system before submitting incident reports. This permits the central computer to

monitor and evaluate the submission of incident reports by each registered user to determine if any particular witness is filing false or misleading reports. For example, if a registered user continually files incident reports containing facts that cannot be verified or confirmed, the central computer may restrict that user's access to the system. The

5　central computer and corresponding program may also calculate and record success rates or validity ratings for each user of the system and post these ratings in the searchable database to enable third parties and the selected authorities to assess the credibility of reports or other information reported by each particular user.

　　　　　　The program may also rate authorities based on their actions or responses

10　to incident reports to encourage them to participate in this system. Users of the system other than authorities may be prompted by the program to rate or indicate their satisfaction level with authorities and this information may be posted on the publicly searchable database to encourage accurate an honest participation by the authorities.

　　　　　　Users may register with the central computer and still remain anonymous

15　by being assigned a code or password. The code or password must be tied to some official identification such as the user's social security number so that the user cannot simply request new codes or passwords; however, the official identification is not provided to others accessing the central computer including the authorities and the other users of the system.

20　　　　　　The central computer 10 and the corresponding computer program may provide private and anonymous communication between users of the system. For example, the system may include e-mail evidence capabilities that enable certified and anonymous communication between users that can be used as evidence to support an incident report or case. To provide accurate witnessing of reports, users who utilize the

25　communication will have their regular e-mail address correspondence detoured through the system so that the central computer can identify the real e-mail address of the users. The central computer and corresponding program may also provide an "action processing interface" that is accessible only by authorities who have registered with the central computer. These authorities can access this interface and add notes and other

30　communications to incident reports to assist the authority that is selected to respond to the incident reports as discussed above. A similar interface may be provided to allow

other participants to add notes and other information to assist the select authority in responding to an incident report.

The central computer 10 preferably records the exact date and time that all incident reports and other data is entered so that the date and time of the information

5 is certified by the central computer. Users may be charged a fee for submitting an incident report. This fee may be charged up-front or deducted from a user's account or shown in the account as due for later payment. Similarly, the system may pay rewards to users for the submission of certain types of incident reports. For example, if the authorities indicate that certain information that was submitted by a user was helpful in

10 resolving a case, the central computer 10 may credit an award to the user's account. This reward may be posted on the central computer 10 before such information is submitted to encourage collection of the information. The rewards may be offered by anyone, including crime victims, authorities, or the operator of the system of the present invention.

15 Although the invention has been described with reference to the preferred embodiment illustrated in the attached drawing figures, it is noted that equivalents may be employed and substitutions made herein without departing from the scope of the invention as recited in the claims.

Having thus described the preferred embodiment of the invention, what is

20 claimed as new and desired to be protected by Letters Patent includes the following: